Secret Network: A Privacy-Preserving Secret Contract & Decentralized Application Platform

Carter Woetzel
www.scrt.network

Abstract. A range of blockchain protocols have enabled a host of decentralized applications and usability based on the programmatic nature of smart contracts and interoperability. Open-source projects have thrived, with rapid adoption of a variety of decentralized internet protocols. A significant portion of the intrinsic value of blockchain is contingent upon immutability and simultaneously the transparency of the underlying ledger.[1] Blockchains that have all data of every smart contract and transaction publicly visible are limited in their capacity to generate effective use cases where privacy is a fundamental component of the feasibility of the application.[2] There has never been a greater need for privacy solutions inside and outside the blockchain space. While transactional privacy has long been a point of focus for a variety of privacy focused protocols, there remains the need for a protocol where the degree to which the underlying data is exposed is programmable by default.[3]

The intent of the Secret Network is to be an open source protocol that enables a wide range of privacy preserving tools and applications through programmable privacy - improving the adoption and usability of decentralized technologies.[4] It is imperative that users in the blockchain domain have accessible alternatives to applications that do not respect their right to privacy. This alternative is made possible by the next generation of smart contracts - Secret Contracts.[5] These contracts enable encrypted input, state, and output allowing for a wide degree of flexibility with both design and implementation decisions.

Protocol

Secret Network is a layer one solution built with the Cosmos SDK, leveraging proof-of-stake (PoS) using Tendermint's Byzantine fault-tolerant consensus algorithms.[6][7] The native token of Secret Network is "SCRT". Computations are performed by each node on the network for verifiability, security, and consensus purposes. Due to being a layer one solution, Secret Network is chain-agnostic and capable of interoperability with a range of networks using the Cosmos InterBlockchain Communication protocol (IBC).[8] To achieve data privacy, the Secret Network protocol leverages key management, encryption protocols, and Trusted Execution Environments

[1] Pilkington, M. (2016, September). *Blockchain technology: Principles and applications* [Scholarly project]. Retrieved from https://doi.org/10.4337/9781784717766.00019

[2] Peng, L., & Feng, W., et. al. (2020, June/July). *Privacy preservation in permissionless blockchain: A survey* [Scholarly project]. Retrieved from https://doi.org/10.1016/j.dcan.2020.05.008

[3] Ibid.

[4] Enigmampc. (n.d.). Enigmampc/SecretNetwork. Retrieved December 20, 2020, from https://github.com/enigmampc/SecretNetwork

[5] Secret Network. (n.d.). Retrieved June/July, 2020, from https://scrt.network/developers/secret-contract-devs/secret-contracts

[6] Kwon, J., & Buchman, E. (n.d.). Internet of Blockchains (Whitepaper). Retrieved December 20, 2020, from https://cosmos.network/resources/whitepaper/en

[7] Unchained, C. (2020, July 21). Tendermint Explained - Bringing BFT-based PoS to the Public Blockchain Domain. Retrieved December 23, 2020, from https://blog.cosmos.network/tendermint-explained-bringing-bft-based-pos-to-the-public-blockchain-domain-f22e274a0fdb

[8] Kwon, J., & Buchman, E. (2019, January 30). Cosmos/cosmos. Retrieved December, from https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md

(TEE) that are part of the hardware specification for all validator nodes of the network. TEEs guarantee that nodes are unable to view computations that occur within the trusted environment - preserving the privacy of the underlying data during the computation. The underlying ledger of Secret Network is publicly visible; the native token SCRT is used for governance, transactions, and gas fees. The protocol implements programmable privacy, which is defined as arbitrarily complex data privacy controls within an application.[9] Programmable privacy enables tokens to be wrapped into their private and fungible equivalent using the Secret Network SNIP-20 standard via a Secret Contract.[10] Blocks are created and appended approximately every six seconds, with a soft limit of approximately twenty-two transactions per second due to a gas per block limit.

Trusted Execution Environments

Just as smart contracts are a trusted neutral party for transactions, in a similar fashion, a Trusted Execution Environment is a neutral party in the form of hardware for secure and private computations. TEEs is hardware that is located in an isolated area on the main processor of a device separate from the main operating system.[11] A TEE ensures that data is stored, processed, and protected in a trusted environment that cannot be tampered with. Using a process of remote attestation, new nodes that are registered on the Secret Network are able to verify the validity of their hardware and TEE.[12] Intel's Software Guard Extensions (SGX) is a set of security-related instruction codes that are built into certain Intel CPUs that enable TEEs.[13] The Secret Network leverages SGX as a TEE. If needed, the protocol can use other TEEs with room for potential future implementations such as secure multi-party computations (MPC).[14] The consensus seed is stored inside the TEE of each validator node, allowing for encrypted inputs to be decrypted and computed across within a safe and secure hardware environment.

Validators

Nodes with a non-negative amount of voting power that secure the network by cryptographically signing blocks are called validators.[15] Block proposals with BFT consensus are done through a series of votes by validators using broadcasted cryptographic signatures.[16] Secret Network's default number of validator nodes is fifty, with room for more nodes to join the network after a modification to the protocol parameters has been agreed upon. Validators earn rewards from transaction fees and block rewards. The more SCRT bonded to any given validator, the greater the

[9] Zyskind, G. (2020, July 14). Programmable Privacy: Turning Smart Contracts into Secret Contracts. Retrieved December 23, 2020, from https://scrt.network/blog/programmable-privacy

[10] SecretFoundation. (2020, November 14). SecretFoundation/SNIPs. Retrieved December 20, 2020, from https://github.com/SecretFoundation/SNIPs/blob/master/SNIP-20.md

[11] Mo, F., Haddadi, H., et. al. (2020, April). *DarkneTZ: Towards Model Privacy at the Edge using Trusted Execution Environments* [Scholarly project]. Retrieved from https://arxiv.org/pdf/2004.05703.pdf

[12] Vill, H. (2017, May). *SGX attestation process - Research Seminar in Cryptography* (1139042598 857914195 P. Pullonen, Ed.) [Scholarly project]. Retrieved December 20, 2020

[13] Intel: Intel Software Guard Extensions, https://software.intel.com/en-us/sgx

[14] Lindell, Y. (2020, June/July). *Secure Multiparty Computation (MPC)*. Retrieved from https://eprint.iacr.org/2020/300.pdf

[15] Kwon, J., & Buchman, E. (n.d.). Internet of Blockchains (Whitepaper). Retrieved December 20, 2020, from https://cosmos.network/resources/whitepaper/en

[16] Ibid.

likelihood said node will be selected for block proposal. Individuals may delegate to validators and earn rewards for bonding a certain amount of SCRT out of active circulation.

Secret Network Bootstrap Process

Before the genesis of a new chain, there must be a bootstrap node to generate network-wide secrets that will empower all the privacy features of the Secret Network chain. When the first node joined the Secret Network, it went through a three-step process.[17] First, the enclave of the bootstrap node generated a remote attestation proof to prove the TEE is genuine. Next, the node generated a random 256 bit number known as the consensus seed. The consensus seed is the most critical part of the Secret Network encryption schema as all other keys and therefore functionality of the protocol are contingent upon secure distribution of this originally generated consensus seed. Using HKDF-SHA256[18] the consensus seed, in combination with other context-relevant data[19], derived private keys for the process of registering a new node, I/O encryption, and state encryption. New nodes also use HKDF-SHA256[20] for key derivation using the original seed or second-generation seeds. Next, the consensus seed is sealed to the disk of the bootstrap node at $HOME/.sgx_secrets/consensus_seed.sealed. Finally, the remote attestation proof, the public key for the consensus seed exchange, and the public key for the consensus I/O exchange are all published to the Secret Network genesis.json. Curve25519[21] is the elliptic curve used for asymmetric key generation and ECDH (x25519)[22] is used for deriving symmetric encryption keys which are used to encrypt data with AES-128-SIV.[23]

New Node Registration

The registration query for a new validator node can be sent to the network consensus layer through SecretCli - the interface for interacting with the network.[24] Components of the registration query consist of the following: a remote attestation proof that the new node's enclave is genuine, a registration public key of the candidate validator node, and a 256 true random nonce. Before these components are sent to the network consensus layer for consensus seed exchange, the candidate node must generate a curve25519[25] curve private/public key pair that will be used for registering the node on the network. Next, using SecretCli the candidate node sends a query[26] to the consensus layer using the previously listed required inputs.

[17] Ibid.
[18] HMAC-based Extract-and-Expand Key Derivation Function (HKDF). (n.d.). Retrieved December 20, 2020, from https://tools.ietf.org/html/rfc5869
[19] HKDF-SHA256 salt which was chosen to be Bitcoin's halving block hash
[20] Ibid.
[21] A state-of-the-art Diffie-Hellman function. (n.d.). Retrieved December 20, 2020, from https://cr.yp.to/ecdh.html
[22] Elliptic-curve Diffie–Hellman. (2020, November 28). Retrieved December 23, 2020, from https://en.wikipedia.org/wiki/Elliptic-curve_Diffie%E2%80%93Hellman
[23] Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES). (n.d.). Retrieved December 23, 2020, from https://tools.ietf.org/html/rfc5297
[24] Zyskind, G. (n.d.). Enigmampc/SecretNetwork. Retrieved December 20, 2020, from https://github.com/enigmampc/SecretNetwork/blob/e0ed66f/docs/protocol/encryption-specs.md#New-Node-Registration
[25] Ibid.
[26] secretclit tx register auth

When the consensus layer receives the registration query transaction from the candidate node, each validator node of the network will verify the remote attestation proof provided by the registration transaction. In order for the consensus seed to be safely transferred to the candidate node, the AES-128-SIV standard is used to achieve this.[27] A seed exchange IKM is derived using ECDH[28] (x25519)[29] using the consensus seed exchange private key and the provided registration public key. Next, a seed exchange key is generated using HKDF-SHA256 using the seed exchange IKM and the previously mentioned HKDF salt as input.[30] Finally, using AES-128-SIV[31] an encrypted consensus seed key is derived using the seed exchange key and the new node's public key as inputs - the consensus seed is the underlying data encrypted. This encrypted consensus seed key is broadcasted to the candidate node. Within the candidate node enclave, all necessary variables required to decrypt the encrypted consensus key are available: the seed exchange key and the new node public key generated previously. Upon decryption of the encrypted consensus seed within the enclave, the consensus seed is then sealed to the disk of said node at $HOME/.sgx_secrets/consensus_seed.sealed. Now that the candidate node has the consensus seed, it can now execute all necessary key derivations to get network-wide secrets in order to participate in block execution and validation.

Privacy Preserving Secret Contracts

Secret Contracts use an adaptation of CosmWasm v0.10 for optimal integration with the Cosmos ecosystem.[32] With CosmWasm, Secret Contracts can run on multiple chains using IBC.[33] Rust is the core language used for the development of Secret Contracts. Rust was chosen due to the convenience of compiling to Wasm as well as resulting optimized runtime performance yielding lower gas costs.[34] Rust's default safeguards against unsafe memory usage and excellent tooling support were additional variables.[35] Secret Contracts enable encrypted input, state, and output.[36] Inputs for Secret Contracts such as block height, time, chain id, sender, address, sent funds, and contract hash are not encrypted.[37] The primary input component that is encrypted is messages created by clients. The contract state (the internal persisted database) of a Secret Contract is always encrypted and only ever known by the contract itself inside the TEE. Outputs that are encrypted are only known to the transaction sender and to the contract itself.

[27] Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES). (n.d.). Retrieved December 20, 2020, from https://tools.ietf.org/html/rfc5297

[28] Elliptic-curve Diffie–Hellman. (2020, November 28). Retrieved December 20, 2020, from https://en.wikipedia.org/wiki/Elliptic-curve_Diffie%E2%80%93Hellman

[29] Elliptic Curves for Security (x5519). (n.d.). Retrieved December 20, 2020, from https://tools.ietf.org/html/rfc7748

[30] HMAC-based Extract-and-Expand Key Derivation Function (HKDF). (n.d.). Retrieved December 20, 2020, from https://tools.ietf.org/html/rfc5869

[31] Ibid.

[32] Enigmampc. (n.d.). Enigmampc/secret-contracts-guide. Retrieved December 20, 2020, from https://github.com/enigmampc/secret-contracts-guide

[33] CosmWasm. (n.d.). CosmWasm/cosmwasm. Retrieved December 20, 2020, from https://github.com/CosmWasm/cosmwasm

[34] Palepu, A. (2019, March 11). Getting Started with Enigma: The Rust Programming Language [Web log post]. Retrieved Winter, from https://blog.enigma.co/getting-started-with-discovery-the-rust-programming-language-4d1e0b06de15

[35] Rust-Lang. (n.d.). Rust-lang/rust. Retrieved December 20, 2020, from https://github.com/rust-lang/rust

[36] Privacy Model of Secret Contracts. (n.d.). Retrieved December 20, 2020, from https://build.scrt.network/dev/privacy-model-of-secret-contracts.html

[37] Ibid.

Queries in Cosmos are unable to cryptographically authenticate the querier's identity; Secret Network solves this by allowing contracts to have an encrypted viewing key that is used to validate the identity of the caller. This viewing key allows for decryption of a range of associated data for any given address. Secret Contracts allowance feature lets accounts designate a portion of their balance to other accounts. This is similar to the allowance feature of ERC-20 contracts, enabling other contracts to manage a portion of the addresses balance. To avoid leaking data, Secret Contracts can enforce constant length messages via padding. The output of transactions can include the following: callbacks to another contract call, a contract init, staking transactions, votes on proposals, instructions for sending funds from the contract's wallet, an error section, and a data section of free-form bytes to be interpreted by the client or dApp with added support for additional types in the future.[38]

Secret Contract State Encryption

While executing a function call inside a TEE of a node as part of a transaction, the Secret Contract code can call the following functions: write_db(field_name, value), read_db(field_name), and remove_db(field_name). Collectively, Secret Contracts' state is stored on-chain inside a key-value store. As such, the field name remains constant between calls. The encryption key for the functional calls uses HKDF-SHA256 from the consensus state IKM, field name, and the contract key. Additional data can also be employed to prevent leaking information about the same value written to the same key at different times. Contract keys are the combination of a signer id as well as an authenticated contract key. The goal of the contract key is to give each Secret Contract a unique and unforgeable encryption key. As a property, unforgeable is imperative to making sure malicious validators are unable to locally encrypt transactions with their own encryption key and then decrypt the resulting state with the fake key. Additionally, each contract must be unique in order to make sure the state of two contracts with identical code are different.

When a contract is initialized from a validator node - inside the node's TEE, a contract key is derived using HMAC-SHA256[39] from the signer id as well as the authentication key. An authentication key is derived using HKDF from an HKDF salt in addition to an IKM that consists of the concatenation of the consensus state IKM and the signer id. Any time a contract execution is called, the contract key of the Secret Contract is sent to every validator node of the network. Upon receiving the contract key, an assertion/check is made to make sure the received contract key matches the expected value.

Theoretical Attacks

Evaluating potential attack vectors is integral to the formation of a protocol that is designed to be the fundamental privacy layer for all blockchain protocols. It is important to note that the majority of theoretical attacks that occur on TEEs (SGX in particular) happen within research labs. In reality, common attack vectors occur through implementation faults that leverage holes in protocol design. Similar to other protocols, decentralization helps secure the network's consensus

[38] Ibid.

[39] HMAC. (2020, December 05). Retrieved December 20, 2020, from https://en.wikipedia.org/wiki/HMAC

layer against Byzantine attacks. As a starting point examining non-consensus layer attacks, these were assumptions made during the design of the Secret Network protocol.[40]

1. Each node is untrusted and is run by a malicious host
2. Each node is equipped with a secure enclave (SGX) that can execute code/data in a trusted manner such that the data cannot be observed or manipulated by the host
3. Assumed PKI (Public Key Infrastructure) and cryptographic primitives are secure (signatures, encryption, etc.)
4. Assumed there is shared consensus in the Secret Network

Here is a list of compiled theoretical attacks:[41]

- Deanonymizing with ciphertext byte count
- Two contracts with the same contract key deanonymize state
- Transaction replay attack
- Search-to-decision millionaire problem
- Partial storage rollback during contract runtime
- Transaction output data leakage
- TEE vulnerability enabling a Byzantine node to acquire the consensus seed from the enclave

Governance

Because Secret Network uses the Cosmos SDK, there is a heavy crossover between other Cosmos protocols and Secret Network with both the design and implementation of governance.[42] Current Secret Network governance parameters, which are subject to change, are as follows:[43]

- Deposit period - 1 week
- Voting period - 1 week
- Minimum deposit amount - 1000 SCRT
- Quorum - 33.4%
- Threshold - 50%
- Veto - 33.4%

There are five stages to on-chain governance proposals with Secret Network: submission, deposits, voting, tallying, and implementation. Submission can be done by any user, with the caveat that nothing is broadcasted on-chain until a proposal reaches the minimum deposit amount.

[40] Guy, & Can. (2020, May 31). Don't trust, verify (an untrusted host). Retrieved December 20, 2020, from https://forum.scrt.network/t/dont-trust-verify-an-untrusted-host/1669

[41] Zyskind, G. (n.d.). Enigmampc/SecretNetwork. Retrieved December 20, 2020, from https://github.com/enigmampc/SecretNetwork/blob/e0ed66f/docs/protocol/encryption-specs.md#Theoretical-Attacks

[42] Cosmos Governance Modules. (n.d.). Retrieved December 20, 2020, from https://docs.cosmos.network/master/modules/gov/

[43] Waugh, J. (n.d.). Secret Network Governance. Retrieved December 20, 2020, from https://scrt.network/blog/secret-network-governance/

This is in place to protect the network from proposal spam. Anyone can contribute to the deposit minimum. If the proposal does not reach the minimum deposit threshold, deposits are refunded. If the proposal is approved or if the proposal is rejected but not vetoed, the deposits will automatically be refunded to the respective proposal depositors. Critical to note is that if a proposal is vetoed with a supermajority, deposits are burned. Upon reaching the minimum deposit required, a one week voting period begins. During this timeframe, bonded SCRT holders are able to cast their vote with one of four options - yes, no, no with veto, and abstain. Only bonded tokens can participate in Secret Network governance; this encourages users to bond their tokens to the network, which is an essential part of securing the network. Voting power is measured in terms of bonded SCRT. Delegators inherit the vote of the validator they are delegated to unless the delegator casts their own vote (which automatically overwrites the validator's voting decision). Tallying the results of a proposal vote can result in an accepted proposal if the following requirements are met: quorum, threshold, and no veto. The quorum requirement programmatically checks that more than 33.4% of total bonded tokens participated in the vote by the end of the one week voting period. The threshold requirement programmatically checks that more than 50% of tokens that participated in the vote, after exclusion of abstain votes, voted in favor of the proposal. The no veto requirement confirms that less than 33.4% of bonded tokens that participated in the vote, after exclusion of abstain votes, vetoed the proposal. Finally, the code the proposal wishes to modify is altered by developers of the network and implemented during the next hard fork of the network - the updated version of the protocol then gets pushed to all nodes supporting the network.

Tokenomics

Secret Network leverages inflation, block rewards, and staking to incentivize SCRT holders and validators to bond their tokens to the network. The less supply that is in circulation, the more difficult it is for a Byzantine actor to successfully execute a Byzantine attack against the Secret Network consensus layer.[44] In addition, in order to drive adoption of the protocol, a generous inflation rate helps pull users, developers, and stakers into the network with the understanding that the inflation rate can be modified in the future through a governance proposal. Secret Network has a variable inflation rate that ranges from 7% - 15% based on the ratio of bonded to unbonded SCRT in relation to the target goal % bonded rate which is 67%.[45] Secret Network has a twenty-one day unbonding period, with a circulating supply of approximately 65 million SCRT and a total supply of approximately 125 million SCRT.[46] Validator nodes can charge a commission rate on delegated SCRT. Currently, the commission rate floor is 0%, with a maximum rate of 20%.[47] The commission rate of validators is only capable of changing by up to 1% every twenty-four hours. Separate from commission rate, there are two additional sets of fees on earned block rewards: the community fee

[44] Lee, S., & Kim, S. (2020, September). *Proof-of-stake at stake: Predatory, destructive attack on PoS cryptocurrencies*. Retrieved from https://dl.acm.org/doi/10.1145/3410699.3413791

[45] Cosmos Inflation Rate. (n.d.). Retrieved December 20, 2020, from https://docs.cosmos.network/master/modules/mint/01_concepts.html

[46] Secret Network Overview: Validators, Governance, and Community Pool. (n.d.). Retrieved December 20, 2020, from https://puzzle.report/secret/chains/secret-2

[47] Puzzle.report: Secretnodes.org. (n.d.). Retrieved December 20, 2020, from https://puzzle.report/secret/chains/secret-2/validators/

(2%) and the Secret Foundation fee (15%).[48] The annual approximate ROI for Secret Network staking ranges between 22% to 27% depending on the validator of choice.[49] The community fee gets pulled from all block rewards and is sent to a pool of funds known as the Community Pool. This pool is used to help fund on-chain governance proposals that help advance the Secret Network ecosystem and protocol. No single entity owns these funds; they are governed in a completely decentralized fashion, empowering the community to voice their opinions and help shape the identity of Secret Network. The Secret Foundation is an organization dedicated to building, researching, and scaling open-source, privacy-centric technologies for the public good.[50] The Secret Foundation helps establish efficient and effective governance practices for the community and the Foundation itself. Additionally, it produces educational content and supports a range of committees that are helping empower individuals and projects created organically within the Secret Network community.[51] The foundation uses its block reward fees to aggressively expand the Secret Network ecosystem which includes direct support for valuable community contributors.

Use Cases

Secret Contracts allow developers to create contracts with control over what subsets of data are encrypted. Due to the completely transparent nature of public blockchains, there has never been a protocol that allows for granular control over data transparency as with the Secret Network protocol. The first proof-of-concept use case to rise to the surface was SafeTrace.[52] SafeTrace is a privacy-preserving contact tracing application that leverages the TEEs of Secret Network to enable summarization of sensitive data, individual high-risk interaction awareness, and data set research empowerment without ever exposing an individual's private data.[53] Computations are run within an SGX enclave, with summary results as output - safeguarding against any single individual's data sovereignty being abused. Next came simple Secret dApps such as SecretPoker and rock-paper-scissors.[54][55] This allows users to play against each other with assurance that no one is able to front-run data or modify decision making due to data that should not be publicly visible within a game environment. Next, the SNIP-20 standard was created which enabled the creation of private, fungible tokens using Secret Contracts.[56] Combining the programmability of ERC-20s[57]

[48] Secret Network: Changes to Inflation Rate and Community Fee. (n.d.). Retrieved December 20, 2020, from https://puzzle.report/secret/chains/secret-2/governance/proposals/16

[49] Woetzel, C., Woetzel, A., & Patla, M. (2020, October). Secret Networking Staking ROI Calculator. Retrieved December 20, 2020, from https://www.securesecrets.network/pages/stakingcalculator.html

[50] Secret: Secret: The Foundation Signal Proposal. (n.d.). Retrieved December 20, 2020, from https://puzzle.report/secret/chains/secret-2/governance/proposals/18

[51] Ibid.

[52] Kisagun, C. (2017, June 17). Enigma and IBM Cloud Are Protecting Human Lives as Well as Data Privacy. Retrieved December 20, 2020, from https://www.ibm.com/cloud/blog/enigma-and-ibm-cloud-are-protecting-human-lives-as-well-as-data-privacy

[53] Enigmampc. (n.d.). Enigmampc/SafeTrace. Retrieved December 20, 2020, from https://github.com/enigmampc/SafeTrace

[54] Enigmampc. (n.d.). Enigmampc/SecretHoldEm. Retrieved December 20, 2020, from https://github.com/enigmampc/SecretHoldEm

[55] Lindlof. (n.d.). Secret Network - Rock/Paper/Scissors. Retrieved December 20, 2020, from https://github.com/lindlof/secret_rock_paper_scissors

[56] SecretFoundation. (2020, November 14). SecretFoundation/SNIPs. Retrieved December 20, 2020, from https://github.com/SecretFoundation/SNIPs/blob/master/SNIP-20.md

[57] Fabian Vogelsteller, V. (2015, November 19). EIP-20: ERC-20 Token Standard. Retrieved December 23, 2020, from https://eips.ethereum.org/EIPS/eip-20

with the privacy of Zcash[58] or Monero,[59] Secret Tokens unlock important use cases and create new value.[60] This allowed tokens not native to Secret Network to be able to gain wrapped privacy properties enabled by Secret Contracts using IBC. Examples of SNIP-20 tokens were secretEthereum, secretDai, secretLink, secretMKR, etc.[61] Secret Auctions are another Secret Contract created in 2020.[62] When a user interacts with an exchange, individuals should be able to query multiple OTC exchanges for their price, and then execute the trade based on the best price.[63] Throughout this entire process, OTC desks shouldn't know each other's bids.[64] If the OTC exchanges are aware of each other's bids then there is potential for collusion against the user. Secret Actions use Secret Contracts to hide this type of vulnerable data in a neutral and programmatic fashion - creating a neutral program that can be trusted by mutually distrustful and privacy-aware entities. Secret Auctions have the potential to turn into Secret Dark Pools which would be a significant contribution to the DeFi ecosystems of the blockchain domain. PadLock helps artists monetize creative work via the decentralized web.[65] Users can buy or sell access to exclusive content hosted on IPFS and Filecoin. The app will generate unique encryption and decryption keys and store them in the encrypted state of a privacy-preserving smart contract on Secret Network.[66] In other words, PadLock uses Secret Contracts to enable programmatic contract interactions that unlock access control via decryption of viewing keys. Secret Non-Fungible Tokens (NFTs) will allow for the creation of NFTs that have verifiable ownership of goods and experiences without ever exposing the underlying owner or their data - all made possible with Secret Contracts.[67] Secret Automated Market Makers (AMMs) will help prevent front-running, a problem that has plagued DeFi since its inception.[68] Due to the public nature of blockchains, front-running attacks happen all the time. Because users can see transactions in the mem-pool and their corresponding gas prices before a block is mined, it is easy for attackers to submit a transaction with a higher gas price, which would result in their own transaction being mined first.[69] The result is an unfairly executed bid or ask with the foreknowledge of the incoming trade - resulting in arbitrage profit due to the modification of supply and demand on a microscale that

[58] Privacy-protecting digital currency. (2020, October 28). Retrieved December 23, 2020, from https://z.cash/

[59] The Monero Project. (n.d.). Retrieved December 23, 2020, from https://www.getmonero.org/

[60] Secret Foundation. (2020, October 22). SecretSCRT: Privacy Tokens are Live on Mainnet! Retrieved December 20, 2020, from https://scrt.network/blog/secret-scrt-privacy-tokens-mainnet

[61] Bair, T. (2020, December 15). The Secret Ethereum Bridge is LIVE on Mainnet! Retrieved December 15, 2020, from https://scrt.network/blog/secret-ethereum-bridge-is-live-on-mainnet

[62] Baedrik. (n.d.). SCRT-sealed-bid-auction. Retrieved December 20, 2020, from https://github.com/baedrik/SCRT-sealed-bid-auction

[63] Kisagun, C. (2020, December 16). Secret Auctions: Towards Decentralized OTC and Dark Pools. Retrieved December 20, 2020, from https://scrt.network/blog/secret-auctions-decentralized-otc-dark-pools

[64] Ibid.

[65] PadlockApp. (n.d.). PadlockApp/padlock-hackfs. Retrieved December 20, 2020, from https://github.com/PadlockApp/padlock-hackfs

[66] Ibid.

[67] Network, S. (2020, October 28). Secret NFTs: Privacy for Verifiable Goods and Experiences. Retrieved December 20, 2020, from https://scrt.network/blog/secret-nfts/

[68] Jack, T. (2020, February 24). Crypto Front Running for Dummies. Retrieved December 20, 2020, from https://parzival-ready.medium.com/crypto-front-running-for-dummies-bed2d4682db0

[69] Kisagun, C. (2020, October 8). Secret Markets: Front Running Prevention for Automated Market Makers. Retrieved December 20, 2020, from https://scrt.network/blog/secret-markets-front-running-prevention/

ultimately the user has to pay for.[70] Because a Secret AMM would keep the mempool private, front-running would be impossible by default.[71]

The use cases of Secret Network will conceivably impact every domain impacted by blockchain. Healthcare, finance, banking, governance, communications, media, supply-chain, voting, identity-fraud, key-access control, exchanges, IoT & mesh networks, forecasting and data set analytics, music and entertainment, real-estate, insurance, wills and inheritance, charity, credit histories, crowdfunding, publishing, gaming, gambling, and messaging. Wherever data privacy needs to be granular and controllable, the Secret Network protocol leveraging TEEs is the programmable privacy de-facto standard for contract development.

History

The Secret Network protocol and community have grown at a breathtaking rate since the launch of Secret Network on February 13th, 2020.[72] Secret Network launched as a proof-of-stake protocol based on Cosmos SDK/Tendermint featuring the native token SCRT.[73] The launch of Secret Network was assisted by 20+ validators looking to support the network. This represented the move towards decentralized governance, sustainability, and a critical step towards making a layer one solution that would enable both scalability and programmable privacy for Web 3.0. The next critical step in the ecosystem occurred in early June with the creation of the Secret Foundation - an organization committed to sustainably promoting the growth of the Secret Network ecosystem.[74] The Secret Foundation did so by advancing privacy as a public good: empowering people by providing tools, technologies, education, and support necessary to preserve their freedom.[75] On June 19th, the Secret Games Incentivized Testnet was announced.[76] Over the course of 56 days (starting on July 20th) there were over 100+ combined participants between the two different test phases. All of these participants played a key role in helping create the future of programmable privacy - secret contracts. In particular, the protocol needed to be stress tested by validator nodes and users in preparation for mainnet upgrade “Vulcan” which would bring Secret Contracts to mainnet after a hard fork of the Secret Network.[77]

On June 24th the burn contract for SCRT was initiated.[78] This burn contract enabled owners of ERC-20 token ENG to convert their cryptocurrency to SCRT — the native token of the Secret

[70] Mitchell, C. (2020, December 14). What Is Front-Running? Retrieved December 20, 2020, from https://www.investopedia.com/terms/f/frontrunning.asp
[71] Ibid.
[72] Enigma Project. (2020, February 19). The Secret Network (Enigma) Mainnet Has Launched. Retrieved from https://blog.enigma.co/the-enigma-mainnet-has-launched-3bd0d40fe80d
[73] Ibid.
[74] Bair, T. (2020, June 15). Introducing Secret Foundation. Retrieved from https://blog.enigma.co/introducing-secret-foundation-4a4598610751
[75] Ibid.
[76] Secret Network. (2020, June 19). Announcing the Secret Games Incentivized Testnet. Retrieved December 20, 2020, from https://scrt.network/blog/announcing-the-secret-games
[77] Woetzel, C. (2020, September 01). Launching Secret Network's Mainnet Upgrade "Vulcan" - A Preview. Retrieved December 20, 2020, from https://caw34769.medium.com/launching-secret-networks-mainnet-upgrade-vulcan-a-preview-a8f3a6d1e8af
[78] Woetzel, C. (2020, December 05). 2020 Deep Analysis of SCRT Burn/Swap - By Secure Secrets. Retrieved December 20, 2020, from https://caw34769.medium.com/2020-deep-analysis-of-scrt-burn-swap-by-secure-secrets-59ea3a6a8d17

Network. Since June 24th, approximately 62 million SCRT had been sent from the burn contract.[79] Importantly, over 35 million SCRT were swapped by Binance on September 29th; Binance was the first major exchange to list SCRT pairs for trading.[80] Overall, the swap was an absolutely resounding success as SCRT gained adoption of governance, staking, and secret contract functionality. An integral part of any ecosystem is the availability of wallets to store and use the native cryptocurrency of the blockchain. Secret Network had early wallet support from both Keplr and MathWallet. Governance proposal #19 saw community pool funding support for Keplr to create a MetaMask UX equivalent for the Secret Network with long term integration and support for Secret Contracts and applications.[81]

On September 15th, 2020 at 14:00:00 UTC the Secret Network successfully hard forked and upgraded the protocol from “secret-1” to “secret-2”. This upgrade enabled Secret Contracts - the core value proposition of the Secret Network. On December 4th, Secret Network officially reached fifty active validators.[82] This was an important milestone for network security, decentralization, and node-onboarding. Along the way to this goal there was an amazing amount of collaboration between validators with a range of experience - all with the shared goal of building a network where programmable privacy is the default for Web 3.0. December 15th, 2020 saw the successful launch of the Secret Ethereum Bridge.[83] This bridge empowered users to wrap Ethereum and fourteen other ERC-20s to their secret SNIP-20 equivalent. To encourage liquidity and adoption, over two million SCRT were offered up as bridge mining rewards.

Philosophy

The Secret Network community is united by a common mission: to advance privacy as a public good, empowering people by providing the tools, technologies, education, and support necessary to preserve their freedom. Fundamentally, we believe privacy is a human right. An overly centralized internet and giant data monopolies have jeopardized our privacy, our security, and our society. We must scale privacy preserving technologies that can help us confront and overcome these systemic risks. We must continue to push for better education surrounding individuals' right to privacy.

Privacy is inextricably intertwined with liberty. In the 21st century data economy there are rarely alternatives that offer a comparable product or experience while preserving users' privacy. Secret Network is the first protocol ever to have a privacy-first, permissionless network for computational privacy; this platform aims to offer up an alternative to perfectly transparent data in the blockchain domain and by extension the world. We believe Secret Network is the privacy sandbox of the future - allowing the sustainable creation of Secret dApps that will permit individuals the freedom to traverse and use Web 3.0 with its full potential realized and

[79] Ibid.
[80] Ibid.
[81] On-chain Proposal. (2020, August 24). Secret Network - Keplr Wallet Integration. Retrieved December 20, 2020, from https://puzzle.report/secret/chains/secret-2/governance/proposals/19
[82] Secret Network (2020, December 4). https://twitter.com/SecretNetwork/status/1334964277673926663
[83] Bair, T. (2020, December 15). The Secret Ethereum Bridge is LIVE on Mainnet! Retrieved December 15, 2020, from https://scrt.network/blog/secret-ethereum-bridge-is-live-on-mainnet

implemented. The guiding principles of our community are usability, sustainability, impact, and empowerment. Every individual is key to the future of Secret Network and privacy. A committed and collaborative community is the most important thing any of us can build - it is the fundamental source for any meaningful change.

We will always push for privacy by default, privacy as an expectation, and privacy as the key to unlocking the full value of a decentralized future.

References

[1] Pilkington, M. (2016, September). Blockchain technology: Principles and applications [Scholarly project]. Retrieved from https://doi.org/10.4337/9781784717766.00019

[2] Peng, L., & Feng, W., et. al. (2020, June/July). Privacy preservation in permissionless blockchain: A survey [Scholarly project]. Retrieved from https://doi.org/10.1016/j.dcan.2020.05.008

[3] lbid.

[4] Enigmampc. (n.d.). Enigmampc/SecretNetwork. Retrieved December 20, 2020, from https://github.com/enigmampc/SecretNetwork

[5] Secret Network. (n.d.). Retrieved June/July, 2020, from https://scrt.network/developers/secret-contract-devs/secret-contracts

[6] Kwon, J., & Buchman, E. (n.d.). Internet of Blockchains (Whitepaper). Retrieved December 20, 2020, from https://cosmos.network/resources/whitepaper/en

[7] Unchained, C. (2020, July 21). Tendermint Explained - Bringing BFT-based PoS to the Public Blockchain Domain. Retrieved December 23, 2020, from https://blog.cosmos.network/tendermint-explained-bringing-bft-based-pos-to-the-public-blockchain-domain-f22e274a0fdb

[8] Kwon, J., & Buchman, E. (2019, January 30). Cosmos/cosmos. Retrieved December, from https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md

[9] Zyskind, G. (2020, July 14). Programmable Privacy: Turning Smart Contracts into Secret Contracts. Retrieved December 23, 2020, from https://scrt.network/blog/programmable-privacy

[10] SecretFoundation. (2020, November 14). SecretFoundation/SNIPs. Retrieved December 20, 2020, from https://github.com/SecretFoundation/SNIPs/blob/master/SNIP-20.md

[11] Mo, F., Haddadi, H., et. al. (2020, April). DarkneTZ: Towards Model Privacy at the Edge using Trusted Execution Environments [Scholarly project]. Retrieved from https://arxiv.org/pdf/2004.05703.pdf

[12] Vill, H. (2017, May). SGX attestation process - Research Seminar in Cryptography (1139042598 857914195 P. Pullonen, Ed.) [Scholarly project]. Retrieved December 20, 2020

[13] Intel: Intel Software Guard Extensions, https://software.intel.com/en-us/sgx

[14] Lindell, Y. (2020, June/July). Secure Multiparty Computation (MPC). Retrieved from https://eprint.iacr.org/2020/300.pdf

[15] Kwon, J., & Buchman, E. (n.d.). Internet of Blockchains (Whitepaper). Retrieved December 20, 2020, from https://cosmos.network/resources/whitepaper/en

[16] lbid.

[17] lbid.

[18] HMAC-based Extract-and-Expand Key Derivation Function (HKDF). (n.d.). Retrieved December 20, 2020, from https://tools.ietf.org/html/rfc5869

[19] HKDF-SHA256 salt which was chosen to be Bitcoin's halving block hash

[20] lbid.

[21] A state-of-the-art Diffie-Hellman function. (n.d.). Retrieved December 20, 2020, from https://cr.yp.to/ecdh.html

[22] Elliptic-curve Diffie–Hellman. (2020, November 28). Retrieved December 23, 2020, from https://en.wikipedia.org/wiki/Elliptic-curve_Diffie%E2%80%93Hellman

[23] Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES). (n.d.). Retrieved December 23, 2020, from https://tools.ietf.org/html/rfc5297

[24] Zyskind, G. (n.d.). Enigmampc/SecretNetwork. Retrieved December 20, 2020, from https://github.com/enigmampc/SecretNetwork/blob/e0ed66f/docs/protocol/encryption-specs.md#New-Node-Registration

[25] lbid.

[26] secretclit tx register auth

[27] Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES). (n.d.). Retrieved December 20, 2020, from https://tools.ietf.org/html/rfc5297

[28] Elliptic-curve Diffie–Hellman. (2020, November 28). Retrieved December 20, 2020, from https://en.wikipedia.org/wiki/Elliptic-curve_Diffie%E2%80%93Hellman

[29] Elliptic Curves for Security (x5519). (n.d.). Retrieved December 20, 2020, from https://tools.ietf.org/html/rfc7748

[30] HMAC-based Extract-and-Expand Key Derivation Function (HKDF). (n.d.). Retrieved December 20, 2020, from https://tools.ietf.org/html/rfc5869

[31] lbid.

[32] Enigmampc. (n.d.). Enigmampc/secret-contracts-guide. Retrieved December 20, 2020, from https://github.com/enigmampc/secret-contracts-guide

[33] CosmWasm. (n.d.). CosmWasm/cosmwasm. Retrieved December 20, 2020, from https://github.com/CosmWasm/cosmwasm

[34] Palepu, A. (2019, March 11). Getting Started with Enigma: The Rust Programming Language [Web log post]. Retrieved Winter, from https://blog.enigma.co/getting-started-with-discovery-the-rust-programming-language-4d1e0b06de15

[35] Rust-Lang. (n.d.). Rust-lang/rust. Retrieved December 20, 2020, from https://github.com/rust-lang/rust

[36] Privacy Model of Secret Contracts. (n.d.). Retrieved December 20, 2020, from https://build.scrt.network/dev/privacy-model-of-secret-contracts.html

[37] lbid.

[38] lbid.

[39] HMAC. (2020, December 05). Retrieved December 20, 2020, from https://en.wikipedia.org/wiki/HMAC

[40] Guy, & Can. (2020, May 31). Don't trust, verify (an untrusted host). Retrieved December 20, 2020, from https://forum.scrt.network/t/dont-trust-verify-an-untrusted-host/1669

[41] Zyskind, G. (n.d.). Enigmampc/SecretNetwork. Retrieved December 20, 2020, from https://github.com/enigmampc/SecretNetwork/blob/e0ed66f/docs/protocol/encryption-specs.md#Theoretical-Attacks

[42] Cosmos Governance Modules. (n.d.). Retrieved December 20, 2020, from https://docs.cosmos.network/master/modules/gov/

[43] Waugh, J. (n.d.). Secret Network Governance. Retrieved December 20, 2020, from https://scrt.network/blog/secret-network-governance/

[44] Lee, S., & Kim, S. (2020, September). Proof-of-stake at stake: Predatory, destructive attack on PoS cryptocurrencies. Retrieved from https://dl.acm.org/doi/10.1145/3410699.3413791

[45] Cosmos Inflation Rate. (n.d.). Retrieved December 20, 2020, from https://docs.cosmos.network/master/modules/mint/01_concepts.html

[46] Secret Network Overview: Validators, Governance, and Community Pool. (n.d.). Retrieved December 20, 2020, from https://puzzle.report/secret/chains/secret-2

[47] Puzzle.report: Secretnodes.org. (n.d.). Retrieved December 20, 2020, from https://puzzle.report/secret/chains/secret-2/validators/

[48] Secret Network: Changes to Inflation Rate and Community Fee. (n.d.). Retrieved December 20, 2020, from https://puzzle.report/secret/chains/secret-2/governance/proposals/16

[49] Woetzel, C., Woetzel, A., & Patla, M. (2020, October). Secret Networking Staking ROI Calculator. Retrieved December 20, 2020, from https://www.securesecrets.network/pages/stakingcalculator.html

[50] Secret: Secret: The Foundation Signal Proposal. (n.d.). Retrieved December 20, 2020, from https://puzzle.report/secret/chains/secret-2/governance/proposals/18

[51] lbid.

[52] Kisagun, C. (2017, June 17). Enigma and IBM Cloud Are Protecting Human Lives as Well as Data Privacy. Retrieved December 20, 2020, from https://www.ibm.com/cloud/blog/enigma-and-ibm-cloud-are-protecting-human-lives-as-well-as-data-privacy

[53] Enigmampc. (n.d.). Enigmampc/SafeTrace. Retrieved December 20, 2020, from https://github.com/enigmampc/SafeTrace

[54] Enigmampc. (n.d.). Enigmampc/SecretHoldEm. Retrieved December 20, 2020, from https://github.com/enigmampc/SecretHoldEm

[55] Lindlof. (n.d.). Secret Network - Rock/Paper/Scissors. Retrieved December 20, 2020, from https://github.com/lindlof/secret_rock_paper_scissors

[56] SecretFoundation. (2020, November 14). SecretFoundation/SNIPs. Retrieved December 20, 2020, from https://github.com/SecretFoundation/SNIPs/blob/master/SNIP-20.md

[57] Fabian Vogelsteller, V. (2015, November 19). EIP-20: ERC-20 Token Standard. Retrieved December 23, 2020, from https://eips.ethereum.org/EIPS/eip-20

[58] Privacy-protecting digital currency. (2020, October 28). Retrieved December 23, 2020, from https://z.cash/

[59] The Monero Project. (n.d.). Retrieved December 23, 2020, from https://www.getmonero.org/

[60] Secret Foundation. (2020, October 22). SecretSCRT: Privacy Tokens are Live on Mainnet! Retrieved December 20, 2020, from https://scrt.network/blog/secret-scrt-privacy-tokens-mainnet

[61] Bair, T. (2020, December 15). The Secret Ethereum Bridge is LIVE on Mainnet! Retrieved December 15, 2020, from https://scrt.network/blog/secret-ethereum-bridge-is-live-on-mainnet

[62] Baedrik. (n.d.). SCRT-sealed-bid-auction. Retrieved December 20, 2020, from https://github.com/baedrik/SCRT-sealed-bid-auction

[63] Kisagun, C. (2020, December 16). Secret Auctions: Towards Decentralized OTC and Dark Pools. Retrieved December 20, 2020, from https://scrt.network/blog/secret-auctions-decentralized-otc-dark-pools

[64] Ibid.

[65] PadlockApp. (n.d.). PadlockApp/padlock-hackfs. Retrieved December 20, 2020, from https://github.com/PadlockApp/padlock-hackfs

[66] Ibid.

[67] Network, S. (2020, October 28). Secret NFTs: Privacy for Verifiable Goods and Experiences. Retrieved December 20, 2020, from https://scrt.network/blog/secret-nfts/

[68] Jack, T. (2020, February 24). Crypto Front Running for Dummies. Retrieved December 20, 2020, from https://parzival-ready.medium.com/crypto-front-running-for-dummies-bed2d4682db0

[69] Kisagun, C. (2020, October 8). Secret Markets: Front Running Prevention for Automated Market Makers. Retrieved December 20, 2020, from https://scrt.network/blog/secret-markets-front-running-prevention/

[70] Mitchell, C. (2020, December 14). What Is Front-Running? Retrieved December 20, 2020, from https://www.investopedia.com/terms/f/frontrunning.asp

[71] Ibid.

[72] Enigma Project. (2020, February 19). The Secret Network (Enigma) Mainnet Has Launched. Retrieved from https://blog.enigma.co/the-enigma-mainnet-has-launched-3bd0d40fe80d

[73] Ibid.

[74] Bair, T. (2020, June 15). Introducing Secret Foundation. Retrieved from https://blog.enigma.co/introducing-secret-foundation-4a4598610751

[75] Ibid.

[76] Secret Network. (2020, June 19). Announcing the Secret Games Incentivized Testnet. Retrieved December 20, 2020, from https://scrt.network/blog/announcing-the-secret-games

[77] Woetzel, C. (2020, September 01). Launching Secret Network's Mainnet Upgrade "Vulcan" - A Preview. Retrieved December 20, 2020, from https://caw34769.medium.com/launching-secret-networks-mainnet-upgrade-vulcan-a-preview-a8f3a6d1e8af

[78] Woetzel, C. (2020, December 05). 2020 Deep Analysis of SCRT Burn/Swap - By Secure Secrets. Retrieved December 20, 2020, from https://caw34769.medium.com/2020-deep-analysis-of-scrt-burn-swap-by-secure-secrets-59ea3a6a8d17

[79] lbid.

[80] lbid.

[81] On-chain Proposal. (2020, August 24). Secret Network - Keplr Wallet Integration. Retrieved December 20, 2020, from https://puzzle.report/secret/chains/secret-2/governance/proposals/19

[82] Secret Network (2020, December 4). https://twitter.com/SecretNetwork/status/1334964277673926663

[83] Bair, T. (2020, December 15). The Secret Ethereum Bridge is LIVE on Mainnet! Retrieved December 15, 2020, from https://scrt.network/blog/secret-ethereum-bridge-is-live-on-mainnet